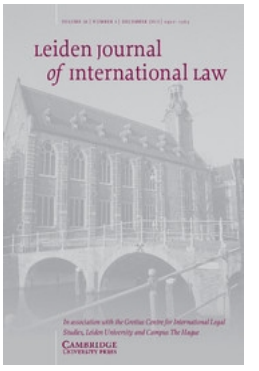
## Expertise, uncertainty and international law, a study of the Tallinn manual on cyberwarfare

Werner, W.G.; Kessler, O.

***published in***
Leiden Journal of International law
2013

***DOI (link to publisher)***
10.1017/S0922156513000410031

***document version***
Publisher's PDF, also known as Version of record




# Expertise, Uncertainty, and International Law: A Study of the Tallinn Manual on Cyberwarfare


OLIVER KESSLER and WOUTER WERNER



Leiden Journal of International Law / Volume 26 / Issue 04 / December 2013, pp 793 - 810
DOI: 10.1017/S0922156513000411, Published online: 08 November 2013

*Leiden Journal of International Law* (2013), 26, pp. 793–810
 doi:10.1017/S0922156513000411

# Expertise, Uncertainty, and International Law: A Study of the Tallinn Manual on Cyberwarfare

OLIVER KESSLER AND WOUTER WERNER*

**Abstract**
How should international law deal with the uncertainty arising from the rise of irregular forms of warfare? In the past decade, this question has been the topic of several reports produced by international groups of experts in the field of conflict and security law. The most recent examples include the study on the notion of the 'direct participation in hostilities' under the auspices of the International Committee of the Red Cross, and the Tallinn Manual on cyberwarfare prepared at the invitation of NATO. In this article, we discuss the Tallinn Manual, showing how experts faced with uncertainty as to the law's precise scope and meaning construct legal interpretations, legal definitions, and institutional facts and norms that can be used to make sense of a contingent world. At the same time, we argue, this absorption of uncertainty produces new uncertainty. Consequently, the power of experts does not reside in their knowledge, but in their control and management of uncertainty and non-knowledge.

**Key words**
cybersecurity; uncertainty; risk; Tallinn Manual; *jus ad bellum*

## 1. Introduction

How should international law deal with uncertainties resulting from the rise of irregular forms of warfare? In the past decade this question has been the topic of several reports produced by international groups of experts in the field of conflict and security law. The most recent examples include the study on the notion of 'direct participation in hostilities' under the auspices of the International Committee of the Red Cross and the Tallinn Manual on Cyberwarfare, prepared at the invitation of NATO.[1] The use of experts to articulate applicable rules of international law is far from novel, of course. The International Law Association, for example, has since 1873 brought together legal experts in an attempt to 'study, clarify and develop'

* Professor of International Relations at the University of Erfurt; International Scholar at Kyung Hee University, South Korea [oliver.kessler@uni-erfurt.de]; and Professor at the VU University, Amsterdam [w.g.werner@vu.nl].

1 Note, however, that the study on direct participation in hostilities was eventually published as a document of the ICRC, because several experts withdrew their names from the project due to fundamental disagreements regarding the interpretation of some key terms of international humanitarian law. The study is available at: www.icrc.org/eng/assets/files/other/icrc-002-0990.pdf. Some other reports dealing with the articulation of law in the area of conflict and security law include the San Remo Manual on International Law Applicable to Armed Conflicts at Sea, the Red Cross Study on Customary Law, or the Harvard Manual on Air and Missile Warfare.

international law.[2] With the establishment of the International Law Commission in 1947 the United Nations formally institutionalized the role of legal experts in the codification and progressive development of international law.[3] Since the Second World War, the institutionalization of legal expertise in the articulation of applicable law has proliferated, as is evidenced by, inter alia, the establishment of the United Nations Commission on International Trade Law or the work of specialized agencies.

The most important task of the recently established committees in conflict and security law is to articulate the applicable international law in a specific (sub)field. The term 'articulate' is chosen deliberately here, as experts are generally not asked to – and do not claim to – make law but instead to articulate the law as it already exists. At the same time experts do more than stating the obvious. Faced with uncertainty as to the law's precise scope and meaning, they construct legal interpretations and inject them with a legitimacy claim based on their expertise. Their aim is to absorb uncertainty by producing interpretations, legal definitions, institutional facts, and legal norms that can be used to make sense of a contingent world.[4]

The increased importance of legal expertise in several functional fields today should not come as a surprise. International law has undergone a process of rapid expansion and increasing specialization, just like law at the domestic level has grown and developed into specialized sub-areas.[5] The net effect of the expansion and specialization of international law has been paradoxical. On the one hand, almost all international decision-making now takes place in a web of legal definitions, legal rules, and legal principles. As the International Law Commission has noted: '[i]t is difficult to imagine today a sphere of social activity that would not be subject to some type of international legal regulation.'[6] This even holds true for the field of international security, a field which has traditionally been regarded as the realm of high politics. As Kennedy has argued, the politics of war today is a politics also fought out in the language of international law; with all participants in armed conflict invoking legal provisions to bolster their cause.[7] On the other hand, the abundance and specialized nature of legal instruments has made it much more difficult to actually know what the law requires – especially for those who are not specialized in a particular legal field. International law is now split up in an ever-growing

2 See www.ila-hq.org (accessed 18 January 18 2013).

3 For a study of the International Law Commission from the perspective of 'legal expertise' see J. S. Morton, *The International Law Commission of the United Nations* (2000). The part on the ILC's mandate for progressive development is interesting when read against the background of legal expertise. Apparently, the General Assembly believed that having legal expertise implies not only knowledge of international law, but also the most reliable opinions for how international law ought to develop.

4 From the perspective of our uncertainty approach, the power of expertise is related to the fixation of meaning in giving structure to uncertainty and turning it into manageable risks. See author for a longer discussion.

5 See the discussion of Habermas's views on law in M. Deflem (ed.), *Habermas, Modernity and Law* (1996).

6 Report of the Study Group of the International Law Commission, Fragmentation of International Law: Difficulties Arising from the Diversification and Expansion of International Law, A/CN.4/L.702, para. 4.

7 D. Kennedy, *Of Law and War* (2006). Anecdotal evidence of Kennedy's point can be found in the complaints by former NATO supreme allied commander Europe, General Jones: 'It used to be a simple thing to fight a battle … In a perfect world, a general would get up and say, "Follow me, men", and everybody would say "Aye, sir" and run off. But that's not the world anymore … [now] you have to have a lawyer or a dozen. It's become very legalistic and very complex.' See L. W. Winik, 'A Marine's Toughest Mission', *Parade*, 19 January 2003, quoting General J. L. Jones, a former NATO commander, explaining how the legalistic nature of today's warfare has complicated the fight.

number of subfields, each with their own norms, rules, precedents, vocabularies, authorities, professional biases, and expert knowledge.[8] Decision-makers are thus called to operate in a legal environment which has become more important than ever before and yet increasingly difficult to disclose. As a consequence, legal experts have become indispensable in many fields of contemporary decision-making and politics. Just like the growth and compartmentalization of scientific knowledge has spurred on calls for experts, the expansion and fragmentation of international law has lifted the role of legal experts in world politics.[9]

The role of international legal experts in different areas has become even more important in light of some foundational challenges to international law. In the field of international security, for example, the rise of issues such as irregular warfare, terrorism, targeted killing, or cyberwar has called into question some constitutive distinctions of peace and security law, including the distinctions between coercion and force, war and peace, combatant and civilian, or military and non-military objects.[10] As Jeffrey Walker has argued in relation to cyberwars:

> Because the entire law of war regime has been built upon a Westphalian foundation, the transformative properties of cyber warfare are just as breathtaking. We are left pondering some fundamental questions … the international legal regime is lagging far behind the problems presented by the increasingly sophisticated technological possibilities in this area.[11]

Bringing such potentially disruptive elements under existing legal categories requires a specific expertise; the knowledge, skills, and imagination of those who are trained and experienced in specific legal fields.

In this article, we reconstruct the role and function of expertise in the case of cybersecurity. This is not a paper on cybersecurity itself, and we do not seek to advance the law of cybersecurity, to demand specific countermeasures, or to develop policy proposals. Rather, we use cybersecurity as an example to reconstruct: (i) how expertise and law are co-constituted in this area by making use of the concepts of uncertainty and risk; (ii) how expert commissions in international law claim authority to articulate the law (and how, if successful, such claims also create new institutional legal facts); (iii) how the use of expertise in conflict and security law may produce new uncertainties or solidify existing doubts regarding the applicability of international law.

We will substantiate our argument by means of a study of the latest expert report in the field of international security: the Tallinn Manual on Cyberwarfare (hereafter the Tallinn Manual). The Tallinn Manual is a good example of the way in which

---

8 M. Koskenniemi, 'The Politics of International Law – 20 Years Later', (2010) 20(1) *European Journal of International Law* 7.

9 For a broader analysis see W. G. Werner, 'The Politics of Expertise: Applying Paradoxes of Scientific Expertise to International Law', in E. Hey (ed.), *The Role of Experts in International Decision Making* (2013, forthcoming).

10 W. G. Werner, 'The Changing Face of Enmity: Carl Schmitt's International Theory and the Evolution of the Legal Concept of War', (2010) 2(3) *International Theory* 351.

11 J. K. Walker, 'The Demise of the Nation-State, the Dawn of New Paradigm Warfare, and a Future for the Profession of Arms', (2001) 51 *Air Force Law Review* 323. Quoted in R. Huges, 'Towards a Global Regime for Cyber Warfare', available at www.ccdcoe.org/publications/virtualbattlefield/07_HUGHES%20Cyber%20Regime.pdf (accessed 18 December 2012).

legal expertise is mobilized in the field of international security. Just like other expert committees in the field, the Tallinn group of experts claims authority on the basis of two different counts: impersonal legal sources and the expertise of the specific persons involved in the project. And just like other expert committees in the field of international security, the Tallinn group is called upon to articulate existing rules of international law in the face of developments that challenge the state-centric foundations of international law. An analysis of the way in which the Tallinn Manual seeks to absorb uncertainty through legal expertise can thus provide useful insights for critical research into the workings of other expert committees in international conflict and security law as well.

In our first section we relate our article to the core topic of this symposium: the co-constitution of legal expertise and its objects. In particular, we will focus on the way in which the securitization of cyberspace has set the stage for specific legal questions and the mobilization of a specific legal expertise. Subsequently, we will discuss how the Tallinn Manual seeks to absorb these uncertainties by recourse to expert knowledge.[12] We will focus on one crucial uncertainty surrounding one of the cornerstones of the UN Charter, the prohibition on the use of force: is it possible to regard cyberoperations as uses of force prohibited by international law? Our article examines how the Tallinn Manual deals with this question. The aim of this examination is not to assess the quality of the Manual or to discuss whether the Manual has provided the right answers to questions pertaining to the use of force. Rather, the Manual functions as a case study to highlight some aspects of the role and function of expertise in international law, with a specific focus on one part of the report, dealing with the use of force.

## 2. The co-constitution of legal expertise and cyberwar

### 2.1. Expertise and the politics of international law

The politics of international law today, Martti Koskenniemi wrote some three years ago, is 'often a politics of re-definition, that is to say, the strategic definition of a situation or a problem by reference to a technical idiom so as to open the door for applying the expertise related to that idiom, together with the attendant structural bias'.[13] The Tallinn Manual on Cyberwarfare provides a good example of Koskenniemi's point. The project was initiated by NATO, chaired by a professor from the US Naval College, and carried out by a group of experts in military affairs and conflict and security law. Not surprisingly, the Manual exclusively deals with cybermatters in terms of applicable *jus ad bellum* and *jus in bello*, taking the reader through an endless list of possible topics that could potentially be relevant for the legal assessment

12 On a more social theoretical level, we thus argue that uncertainty reduction goes hand in hand with uncertainty production. One cannot have one without the other. What the manual does, however, is to transform unstructured into structured uncertainty, and thereby stabilize the meaning and applicability of the legal vocabulary (and imagination). The source of uncertainty is related to the uncertainties generated by cyberspace, which are framed in terms of risks. The Tallinn Manual reduces these uncertainties by invoking the legal vocabulary centered around norms. The 'structured' uncertainties result from the conflicts arising from bringing risks under the heading of norms.

13 See Koskenniemi, *supra* note 8, at 11.

of cyberwar, including what look like slightly exotic topics such as the protection of medical and religious personnel, *levée en masse* (making the reader wonder what that would look like in cyberspace ...) or the abuse of the UN emblem.[14]

While the list of topics studied under the rubric of conflict and security law is lengthy indeed, the report is of course also limited in that it focuses on those areas of law that are of specific interest for NATO (thus leaving aside other possibly relevant areas such as human rights, *lex digitalis*, criminal law, or international economic law). The framing of cyberspace in terms of conflict and security law is partly the result of a longer-term process wherein states and international organizations have focused on (potential) threats that emanate from the world of cyber. At the same time, discussing problems in cyberspace through the lens of conflict and security law reconstitutes the very nature of the topics under consideration. Cyberoperations become 'uses of force', 'self-defence operations', 'aggression', or 'armed attacks' while agents are reconstituted as 'combatants' and 'civilians'. The Tallinn Manual is thereby also exemplary of the central topic for this symposium as identified by the editors' introduction, the co-constitution of legal expertise and their objects. Rather than standing 'in-between the production and application of knowledge' as a well-known definition of expertise would have it,[15] legal experts are products and co-producers of their object of study and advice.[16] As a result, the Tallinn Manual can be read in two ways. First, as the product of a longer trend in which the object of 'cyber' is phrased and constituted in terms of 'uncertain threats' to which military responses could (or should) be considered (section 2.2 below). In this sense, the socially constructed object of cybersecurity constitutes specific groups of individuals as experts. Second, as an attempt to absorb the uncertainties surrounding cyberwar through legal reasoning and the application of rules (section 2.3), an attempt that, as we will show in section 3, paradoxically solidifies some of the uncertainties surrounding the application of existing law to cyberwar.

### 2.2. Uncertainties of cyberspace

In order to obtain a sense of the social construction of cyberspace as an area of insecurity and unpredictability,[17] it is useful to remember that cybersecurity has a history that goes back at least to the mid-1970s, when distant access for entering programs and data became possible and when cybersecurity already became part of the US national security agenda.[18] In its over-35-year history, the debate and

14 See Tallinn Manual, respectively, under Rules 70–3, 27, and 63.

15 N. Grundmann and R. Stehr, *Experts: The Knowledge and Power of Expertise* (2011), at 40, describing experts as 'mediators between producers of knowledge and users of knowledge; and thus, between those who create the capacity to take action and those whose task it is to act'.

16 In other words, the co-constitution of expertise and field of study runs through the stabilization of imaginations.

17 The objective of this section is neither to provide a complete overview of the history of cybersecurity, nor to provide a comprehensive account of all aspects of cybersecurity. This section simply reconstructs the extent to which transformative dynamics associated with cybersecurity trespass traditional legal confines and at the same time calls for 'new' legal expertise.

18 M. Dunn Cavelty, *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age* (2008), at 45, 54, and M. Dunn Cavelty, 'From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse', (2013) *International Studies Review* 15(1), at 109.

dominant images have shifted.[19] We do not want to reiterate the history of cybersecurity itself, but rather point to three distinct sources of uncertainty: (i) the blurring of previously believed solid distinctions like public and private; inside and outside; (ii) the (alleged) novelty of cyberthreats, including the difficulties in attributing them to actors; and the (iii) lack of historical experience and reliance on analogies and metaphors.[20]

First, cyberthreats trespass the classic confines of public international law. For example, in the aftermath of the Oklahoma City bombing in 1995, the debate on cybersecurity in the US moved from the hackers and foreign intelligence to critical infrastructure. In the aftermath of the bombing, President Clinton set up the Presidential Commission on Critical Infrastructure Protection that presented its results in 1997 and made clear that modern societies depend on the functioning of critical infrastructures like electricity, telecommunication, or financial services. Its report on 'Critical Foundations: Protecting America's Infrastructure'[21] opened by making clear that:

> Our national defense, economic prosperity, and quality of life have long depended on the essential services that underpin our society. These critical infrastructures – energy, banking and finance, transportation, vital human services, and telecommunications – must be viewed in a new context in the Information Age. The rapid proliferation and integration of telecommunications and computer systems have connected infrastructures to one another in a complex network of interdependence. This interlinkage has created a new dimension of vulnerability, which, when combined with an emerging constellation of threats, poses unprecedented national risk.[22]

Critical infrastructure protection showed that threats do not fit into traditional categories such as the distinction of private/public, as the providers of those infrastructures now find themselves to be part of a security discourse. The classic distinction between public and private actors consequently gets blurred when, for example, energy providers find themselves to be part of a security discourse. In addition, critical infrastructure protection shows that contemporary threats are linked to the very characteristics of the infrastructures over which the state does not have complete control. Apart from the necessary inclusion of other actors in the security discourse, these security threats do not emanate from 'outside' one's own territory. This means that the classic distinction between inside and outside upon which

19 See Dunn Cavelty (2008), *supra* note 18, for a detailed discussion.

20 The reason for focusing on these three uncertainties – without neglecting other sources or understandings of uncertainties – relates to the fact that all these three sources of uncertainty make a classic use of the law of war problematic.

21 The report is available at www.cyber.st.dhs.gov/docs/PCCIP%20Report%201997.pdf. For a discussion on critical infrastructure, see G. Giacomello, 'Bangs for the Buck: A Cost–Benefit Analysis of Cyberterrorism', (2004) 27(5) *Studies in Conflict and Terrorism* 387; G. Weimann, *Terror on the Internet: The New Arena, the New Challenges* (2006). M. Dunn Cavelty and K. Soby Kristensen (eds.), *Securing the Homeland: Critical Infrastructure, Risk, and (In)Security* (2007).

22 US President's Commission on Critical Infrastructure Protection 1997, available at www.cyber.st.dhs.gov/docs/PCCIP%20Report%201997.pdf, at ix.

classic legal categories are based is called into question.[23] As an answer to these uncertainties, the report called for proactive measures, as:

> while we see no electronic disaster around the corner, this is no basis for complacency. We did find widespread capability to exploit infrastructure vulnerabilities. The capability to do harm – particularly through information networks – is real; it is growing at an alarming rate; and we have little defense against it.[24]

The second source of uncertainty relates to the difficulties of identifying the agents responsible for cyberattacks (or what were sometimes called acts of 'cyberterrorism').[25] This can be illustrated by the classical examples of Estonia (2007) and Georgia (2008)[26], Iran (2010), or the Red October virus. In all these cases there was not only doubt as to whether the attacks constituted examples of espionage, intervention, the use of force, or an armed attack in the legal sense; there were also questions whether the attacks could be (legally) attributed to an identifiable agent.[27]

After Estonian officials decided to relocate a memorial of the Soviet liberation from the Nazis, a cyberattack paralysed the entire Estonian infrastructure on 30 April. Additionally, many official Internet sites became temporally unavailable (a distributed denial of service (DDoS) attack). There were strong indications that the attack originated from Russia, but there was no solid proof of the source of the attacks.[28] Additionally, during the Georgian war in 2008, several DDoS attacks

---

23 For a longer discussion, see S. J. Collier and A. Lakoff, 'The Vulnerability of Vital Systems: How "Critical Infrastructure" Became a Security Problem', in Dunn Cavelty and Soby Kristensen, *supra* note 21. See also G. L. Herrera, 'The Politics of Bandwidth: International Political Implications of a Global Digital Information Network', 2002 28(1) *Review of International Studies* 93; see also www.blog.internetgovernance.org/blog/_archives/2011/9/20/4903371.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A±IGPBlog±%28IGP±Blog±Main%29.

24 See President's Report, *supra* note 22, at 34.

25 Soon after the President's Report in 1997, the word 'cyberterrorism' was introduced and gained widespread attention with the terrorist attack on 11 September 2001. See Dunn Cavelty, *supra* note 18, 101. The idea that terrorist groups could use the cyberspace to launch an attack from anywhere in the world (including from within the US itself) was not too far away from what has happened on 9/11. Even though, as Dunn Cavelty argues, the Bush Administration actually followed Clinton's frames, the US The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act expanded the range of cyberterrorism extensively: what was previously treated as cybercrime could now easily be reinterpreted as acts of terrorism.

26 See in particular R. Deibert, J. Rohozinski, and M. Crete-Nishihata, 'Cyclones in Cyberspace: Information Shaping and Denial in the 2008 Russia–Georgia War', (2012) 43(3) *Security Dialogues* 3. They point out that the C&C servers responsible were located on Russian territory, but appear to originate from a private company. Also, see J. Bumgarner and S. Borg, 'Overview by the US-CCU of the Cyber Campaign against Georgia in August 2008', available at www.registan.net/wp-content/uploads/2009/08/US-CCU-Georgia-Cyber-Campaign-Overview.pdf. See also www.worldaffairsjournal.org/article/shadow-wars-debating-cyber-disarmament.

27 See for example www.erratasec.blogspot.de/2012/09/there-was-no-georgia-cyber-war.html (last accessed on 13 May 2013). The point here is not to call into question the existence of DDoS attacks or to deny Russia's involvement, but to simply point out that attribution is difficult if, for example, a government-owned computer can be 'hijacked' by a hacker and manipulated. There is simply uncertainty around who is to be held responsible for an attack and under what conditions it can be attributed to a state.

28 Given the tensions between Estonia and Russia right before the attack, Russia was accused of standing behind these attacks. See www.spiegel.de/international/world/old-wars-and-new-estonians-accuse-kremlin-of-cyberwarfare-a-483394.html (last accessed on 13 May 2013). Eventually a 20-year-old student was thought to be responsible for the attack. The fact that Estonia is part of NATO might explain why NATO has a specific interest in clarifying the status of 'cyberwar' for its own Art. 5.

on Georgian websites were reported; again there were indications but no definite proof that a state-sponsored agent was responsible for the attack. The debate shifted considerably with the discovery of Stuxnet in June 2010. Stuxnet was a worm that was initially targeted at Siemens supervisory control and data acquisition systems (STADA) and was employed to sabotage the Iranian nuclear programme. Rumour suggested that US and Israeli intelligence were behind this attack.[29] Yet rumours and articles in mass media are not considered evidence in the legal sense. Again, it proved hard to trace down the origin of a virus. And even if the originator is found, it could be a private company or a specific individual, with all the problems that arise in terms of attribution and state responsibility under international law.[30]

A third example is the debate surrounding the virus called 'Red October'.[31] Red October was active for over five years, operational in over 60 countries, and able to extract classified information.[32] It used computers and mobile phones from embassies, government agencies, multinational corporations, nuclear and military sites, and research centres around the globe.[33] The virus traced data that was encrypted with specific codes (like Acid Cryptofiler, which is used by the EU and NATO) and was controlled by a chain of over 60 so-called command-and-control (C&C) servers. This chain makes it, given current knowledge, impossible to trace down the origin of the virus, or to identify its mastermind. It was unclear what the virus tried to do, what the information was for, and who wanted to accomplish what with the virus. If cyberspace allows for new ways to hide or even erase origins, then this makes any simple 'translation' into the legal vocabulary of 'attribution' virtually impossible.

The third source of uncertainty relates to the lack of historical experience: there is a widespread consensus in the literature that – Stuxnet notwithstanding – there simply has been no incident of a cyberwar that inflicted the widespread devastation and damage usually associated with 'war'. If we associate war with severe damage and a significant number of dead bodies, then this has simply not yet happened. Of course, the Georgian war was flanked by cyber attacks, but the cyber attacks themselves did not create severe enough damage to legitimize the use of the concept of 'war'.[34] Assessing the legality of responses to cyber attacks thus remains to a large extent a matter of speculation and hypothetical reasoning. In this context it is quite telling that imminence and urgency are created through analogies like 'electronic Pearl Harbor' and not through historical reconstructions. The Tallinn Manual also

29 See www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all&_r=0 (last accessed 10 May 2013).

30 As Deibert, Rohozinski, and Crete-Nishihata, *supra* note 26, point out, cyberspace is now considered equally important as 'traditional' areas of land, air, sea, and space. At the time of writing, there are news reports that the US army has quadrupled its cybersecurity capacity.

31 See www.telegraph.co.uk/technology/news/9800946/Red-October-computer-virus-found.html (accessed 10 May 2013). Even though Red October is more a case of cyberespionage than cyberwar, it highlights the difficulties of attribution.

32 Because the virus remained undetected for years and used new techniques that made it 'silent' (at least for common antivirus alert systems), experts labelled the new virus 'Red October', in memory of the USSR submarine in the Hollywood movie.

33 For a map of infected countries, see www.spiegel.de/international/spiegel/how-russian-virus-hunters-tracked-down-a-global-espionage-network-a-879467.html.

34 Rule 13, para. 13.

attests to this by pointing out that 'no international cyber incidents have, as of 2012, been unambiguously and publicly characterized by the international community as reaching the threshold of an armed attack'. Yet although a cyberwar appears to be unlikely – given the necessary means and the expected damage it could produce – cybersecurity is meanwhile regarded to be as important as other areas of security. In this context it is important to note that issues of cyberspace are increasingly discussed in terms of a 'preventive logic'. [35]

### 2.3. Uncertainty and legalization

With the imaginaries of cyberspace in terms of danger, risk, and uncertainty in place, the framing of the issues relating to cyberspace in the Tallinn Manual did not come as a surprise.[36] The experts had to apply existing law to an object that had already been imagined in terms of unpredictability and danger for more than a decade. In that sense it was the object that to a large degree determined the applicable law: if analogies can be drawn to Pearl Harbor, it becomes almost a matter of course to assess cyberspace in terms of conflict and security law. In addition, questions regarding the applicability of international law to the phenomenon of cyberspace had been raised repeatedly: was it possible to frame the issue of cyberwar in established terms such as 'state responsibility', 'use of force', 'armed attack', 'military object', and 'combatant'? In this sense the Tallinn Manual can be seen as an attempt to define and constitute the object in terms of the legal expertise involved.

However, there is by definition a tension between framing issues in terms of danger, threats, and insecurity, and attempts to define objects in terms of pre-existing rules and principles. A successful presentation of cyberspace as a realm of insecurity, uncertainty, and threats to critical infrastructure almost naturally comes with resistance to a legalistic ethos that seeks to subject political decision-making to general and pre-given rules.[37] The logic of uncertainty and prevention that characterizes many security policies on cyberspace sits uncomfortably with the idea that decision-making should be based on pre-existing legal norms and principles.[38] The logic of legalism, by contrast, is one of recourse to a system of rules 'out there' that can be applied to matters at hand.[39] A legalistic approach attempts to define matters as subject to the normal operation of rules: although sometimes the creativity of legal minds is called for, it is possible to define the world in terms of the pre-given

35 Even though we generally agree with Dunn Cavelty (2008) that the history of cybersecurity is a history of failed securitization moves and can rather be understood in terms of 'threat politics', this contribution differs from the literature on securitization, critical infrastructure, or threat politics insofar as it is interested in the constitution of legal expertise and not the security experts. However, we do agree that the representation of the 'object' is crucial to understanding the kind of knowledge claims put forward and the form of legitimate expertise.

36 Even though we talk about (existential) threat here, we do not follow the securitization approach. For a discussion see L. Hansen and H. Nissenbaum, 'Digital Disater, Cyber Security, and the Copenhagen School', (2009) 53 *International Studies Quarterly* 1155.

37 For an excellent discussion of legalism as the ethos of the legal profession see J. Shklar, *Legalism* (1964). We also thank a reviewer for pointing out the conflict between successful securitization and legalization.

38 For an interesting juxtaposition of the logics of risk and legal responsibility see F. Ewald, *L'état providence* (1986).

39 See Shklar, *supra* note 37.

standards, rules, and principles that law provides. The Tallinn Manual operates within this tension, with an object that for over a decade has been defined as potentially dangerous, irregular, and requiring action based on a logic of prevention and risk; and at the same time the ambition to apply pre-given rules of positive conflict and security law. The text takes the reader through all the well-established known categories of the UN Charter and humanitarian law, making admirable efforts to apply the normalcy of law to the irregularity of dangers emanating from cyberspace. Seen in this light, the ambition of the Manual is almost breathtaking. In the words of the chairman of the Tallinn group of experts, Michael Schmitt, the idea behind the Tallinn Manual was not 'to bring a bunch of lawyers together … who appear to impress the audience by telling how truly hard cyber is'.[40] What about, Schmitts wonders, 'if we start answering the questions?'[41] In other words: the idea behind the Manual was answering questions that the newly constituted object of cyberwar produced, in terms of positive international law. Below we will turn to the way in which the group of experts asserted its own authority to tackle the ambitious task of defining cyberwar in terms of existing international law.

## 3. International legal expertise and uncertainty reduction

### 3.1. The question of authority and the composition of the expert group

The use of expert knowledge is generally meant to provide a specific form of legitimacy or authority for certain interpretations, decisions, or arguments (or, of course, to undermine their authority). The legitimacy bonus of expert knowledge is derived from two somewhat contradictory elements. On the one hand, expert knowledge consists of an impersonal validity claim; for expert knowledge to work, it should present itself as independent of the personal preferences of the expert in question. If an expert fails to convince an audience that the knowledge she produces is independent of her personal likes or dislikes, her claim to expertise will most likely fail. On the other hand, the power of expert knowledge is rooted in the specific position and reputation of the expert in question.[42] It is not just any person making a validity claim; it is persons who have specific skills, knowledge, and experience who make the claim. In this sense it matters a great deal whether one person or the other is attempting to produce expert knowledge.

---

40 The quotes are taken from a presentation by Michael Schmitt on the Tallinn Manual CyCon 2012. M. Schmitt, 'Tallinn Manual Part I', posted at youtube: http://www.youtube.com/watch?v=wY3uEo-Itso (0:40).

41 See *supra* note 40, at (0:50).

42 This raises the question how disciplinary knowledge – and the boundaries it sets – constitute certain power relations and make expertise possible. Apart from questions of representation and legitimation (who elected the bankers? Or the lawyers?), this constitutes also a fight between these disciplines over issue areas, a problem we cannot deal with in further detail at this point. However, it does raise the question through which practices, concepts, and images 'law' allows for certain 'experts', and how these experts have to relate to law in a specific way to count as experts. This boundary then also sets the boundary of critique – because not every critique will be taken into consideration. See O. Kessler, 'Beyond Sectors, Before the World: Finance, Security, and Risk', (2011) 42(2) *Security Dialogue*, 197.

The ambiguous basis of expert knowledge is also visible in the Tallinn manual. The Manual takes great pains to set out that it is not meant to represent the position of states or international organizations on the law applicable to cyberwar. Instead, it sets out to explicate existing international definitions, rules, and principles of law as they can be found in established sources of international law. The long and impressive list of legal sources and authorities included in the very beginning of the report attests to this. Although the Manual acknowledges that different interpretations are possible (and openly discusses differences of opinions throughout the report), its claim to validity is thus based on pre-given sources such as treaties and customary law.[43] The claim of the report, in other words, is that anyone following the proper methods of international law would come to (more or less) the same results. At the same time, the report cannot but acknowledge that it has specific origins as well as a geographical bias. In addition to the international legal sources that allegedly enjoy validity for all states, the report heavily draws on the military manuals of four states (Canada, Germany, the United Kingdom, and the United States), because 'the international community generally considers these four manuals to be especially useful during legal research and analysis with respect to conflict issues'.[44] The wording is chosen carefully in order to prevent the manuals of four NATO states being put on a par with primary legal sources that bind all states alike: the manuals are considered 'especially useful', not a direct source of authority. Yet, the way in which primary legal sources are to be read and applied in context can be inferred from the four manuals, because 'the international community' apparently finds them useful in legal research and analysis. In this way, the four manuals are injected with global authority that transcends their geographical, political, and cultural boundaries.

Given the history of the laws of armed conflict international law (and international law in general), it is somewhat remarkable to see that the Manual moves seemingly smoothly from the opinions of a few Western states to the 'international community' as a whole. As Megret has noted, international humanitarian law today is still closely tied to nineteenth-century, Western images of legitimate statehood and the corresponding understandings of international law's nature and function. Whereas most international lawyers will see the function of humanitarian law primarily as regulating warfare, 'the realist, the underdog or the anti-colonialist might well all tell a different story, one in which the role of the laws of war is above all to reinforce the state's unshakeable stranglehold and express the dominant consensus about the state's incontrovertible legitimacy'.[45] Now it would certainly be far-fetched and unfair to label the Tallinn Manual a product of neo-colonialism. However, it is interesting to note that it does encounter problems that are not dissimilar to the ones raised in postcolonial scholarship.[46] The close ties between conceptions of statehood that prevailed in the nineteenth century and international

43 See *supra* note 26.
44 See *supra* note 26, at 21.
45 F. Megret, 'From Savages to Unlawful Combatants: A Postcolonial Look at International Law's "Other"', in A. Orford, *International Law and Its Others*, 265, also available at http://people.mcgill.ca/files/frederic.megret/Megret-SavagesandtheLawsofWar.pdf, at 29.
46 Ibid.

law's understanding of war also make it difficult to make sense of operations taking place in and through cyberspace, operations that are increasingly portrayed as trespassing established legal boundaries.

However, the report does not only ground its validity claims in legal sources. It also invokes the specific position and reputation of the experts involved in order to convince the audience.[47] Take, for example, the way in which the report grounds its conclusions regarding the validity and scope of customary international law: 'Ultimately, the professional knowledge, experience, and expertise of the Experts form the basis for the Tallinn Manual's conclusions as to the customary status of a Rule or its extension into non-international armed conflict'.[48] The authority of the report is thus grounded not only in sources of international law, but also in the trust we should have in the professional knowledge, expertise, and experience of Experts (with capital E). The report explicitly underlines this by stating that the group of experts is composed of experienced practitioners, 'world-class expert' academics, and technical experts: a mix that 'is crucial to the credibility of the final product'.[49]

In this context it is important to underline the way in which the experts were selected. The process started with an invitation of the NATO Cooperative Cyber Defense Center of Excellence to Michael Schmitt, asking him to put together a group of experts that could start answering questions regarding the applicability of international law to matters of cyberwar. As such, the fact that Michael Schmitt was invited to chair the group of experts for the NATO Center is not very surprising. Schmitt had acted as a member of expert committees before,[50] is chair of the international-law department at the US Naval War College, and is the author of some innovative and widely quoted articles on cyberwarfare.[51] Schmitt's earlier work on cyberwar – and on international humanitarian law in general – combined two elements that fitted the idea of a manual on the applicability of international law to cyberwar particularly well. First, Schmitt had repeatedly argued that existing international law covers new developments in military technology, although the application of law to new problems may require the craftsmanship and creativity of professional lawyers. According to Schmitt, issues such as drone warfare or cyberwar do not take place in a legal vacuum but in a pre-existing system of rules whose exact meaning can be established through legal interpretation.[52] What is needed, therefore, is not the adoption of new legal instruments (as some have argued) but the (re)interpretation

47 This audience encompasses policy makers and security experts but also the discipline of 'international law'. Hence 'audience' in our understanding relates to the problem of 'the public'.

48 Ibid., at 20–1.

49 Ibid., at 22.

50 Schmitt was one of the experts that took part in the deliberations on the ICRC study on civilians directly participating in hostilities. Schmitt, however, was one of the experts that disagreed so fundamentally with the propositions contained in the ICRC's Interpretative Guidance that he asked to delete his name as one of the participants. Schmitt basically disagreed with the way in which the ICRC study struck the balance between humanity and military necessity.

51 The debate on the legal aspects of cyberwar took off after M. Schmitt, 'Computer Network Attacks: Thoughts on a Normative Framework', (1999) *Columbia Journal of Transnational Law* 37, 885.

52 'Yet, cyberspace is not a lawless firmament. As with the aforementioned weapons, the established norms … govern their use', in M. Schmitt, 'Cyberspace and International Law: The Penumbral Mist of Uncertainty', (2013) *Harvard Law Journal* 126, 176–89, at 176.

of the international legal framework already in place. Or, as Schmitt has put it in an interview with ABC News: 'Let's be honest. Everyone has treated the Internet as a sort of Wild West, a lawless zone. But international law has to be just as applicable to online weapons as conventional weapons'.[53] Second, his work is based on the (widely shared) assumption that international law is ultimately made, applied, and enforced by states.[54] This statement is echoed in the Manual's repeated assurances that the experts by no means create new rules of international law, but only state and clarify what states had already agreed on. More specifically, Schmitt had taken the position that international humanitarian law 'must remain sensitive to the interest of states in conducting warfare efficiently'; a position that made it more likely that his chairmanship would prevent the adoption of guidelines that were far removed from the will and interests of the NATO states.[55]

The invitation to Schmitt came with a blank cheque: he was given as much money as he needed and complete freedom to design his own group of experts.[56] There will be few people doubting that the group that Schmitt eventually composed contained highly competent lawyers, technical experts, and practitioners. At the same time, however, the group reflects a geographical bias[57] and does not include critics of the positions earlier adopted by the chair. The Manual itself also remains silent about the criteria that were used to select the most relevant 'professionals, technical experts and world class academics'. Given the relatively underdeveloped nature of the international legal discipline in terms of journal ranking and impact assessment, it is probably virtually impossible to set any fixed criteria for who counts as world-class academics and who allegedly operates at a different level. Yet, the selection of experts is very important in light of the statement that the group of experts has sought to 'capture all reasonable positions for inclusion in the Tallinn Manual's Commentary'.[58] The implicit argument that is made here is that legal positions not mentioned in the Manual are apparently 'unreasonable' in the eyes of the experts. Anyone who would like to bring such 'unreasonable' arguments to the fore will have to argue against the authority of the assembled experienced practitioners, 'world-class expert' academics and technical experts.

The mere fact that an internationally constituted group of experts manages to present consensus on some legal issues is likely to be taken up as a powerful signal in the popular press, in academia, and in political circles. In the case of the Tallinn Manual, its findings were presented in the media as a 'new doctrine' with possibly

53 Available at www.abcnews.go.com/International/arming-virtual-battle-dangerous-rules-cyberwar/story?id=18888675&page=2.

54 M. Schmitt, 'The Interpretative Guidance on the Notion of Direct Participation in Hostilities: A Critical Analysis', (2010) 1 *Harvard National Security Journal* 5, at 7.

55 Ibid., at 6. Note that Schmitt's reliance on international law as a pre-existing system and his assumption that international law stems from the will and interests of states reflects the mainstream international law position identified by M. Koskenniemi, *From Apology to Utopia* (2005). This raises again questions about attribution in the context of cybersecurity.

56 See *supra* note 40, at (1:10).

57 On this point see *infra*, p. 803.

58 See *supra* 26, at 20.

dangerous implications,[59] as an 'attempt at codification' and a 'handbook',[60] as 'the likely key reference' when states would decide to adopt rules for conflict in cyberspace,[61] or as 'in short … the new rules of war for a new type of war'.[62] In addition, the Manual was embraced by one of NATO's legal assistants as 'the most important document in the law of cyber-warfare'.[63] While it is too early to tell how the Manual will or will not affect the position of states, it is interesting to note that the chair of the expert groups has already made an attempt to portray the findings of the Tallinn Manual as basically reflecting the *opinio juris* expressed by the United States. According to Schmitt, the *opinio juris* of the US could be deduced from a public speech on international law and cyberspace by US State Department Legal Advisor Harold Koh.[64] The congruence between the US position and the Tallinn Manual, Schmitt argues, 'is striking. This confluence of a state's expression of *opinio juris* with a work constituting "the teachings of the most highly qualified publicists of the various nations" significantly enhances the persuasiveness of common conclusions'.[65]

Now, as may be expected, the experts did not reach consensus on all legal issues, and, in particular, not on some foundational questions of *jus ad bellum* and *jus in bello*. Given the potential impact of the Manual it is important to study the possible consequences of such a failure among experts to produce consensus on the application and interpretation of rules. As has been observed in relation to scientific expertise, a lack of consensus can eventually be detrimental to the authority claims put forward by experts and expert committees.[66] In this context, it is possible to identify at least two different ways in which experts can fail to produce clear consensus on the scope and interpretation of rules.

In the first place, expert reports can produce 'officially notified disagreement' in cases where experts have irreconcilable views on the best way to read particular provisions. When experts disagree on the reading of a rule, this sends a signal to legal and political communities that experienced and knowledgeable experts acknowledge that different and maybe even contradictory interpretations are all reasonable. While this reduces complexity because not all positions are recognized as acceptable, it also officially stamps the existence of uncertainty surrounding

59 See ABC News, 'Arming for Virtual Battle: The Dangerous New Rules of Cyberwar', 7 April 2013, at www.abcnews.go.com/International/arming-virtual-battle-dangerous-rules-cyberwar/story?id=18888675&page=3.

60 See 'Rules of Cyberwar: Don't Target Nuclear Plants or Hospitals, Says Nato Manual', *Guardian*, 18 March 2013, available at www.guardian.co.uk/world/2013/mar/18/rules-cyberwarfare-nato-manual.

61 M. Mimoso, *Tallinn Manual Interprets International Law in Cyberwar Context* (25 March 2013), available at www.threatpost.com/tallinn-manual-interprets-international-law-cyberwar-context-032513.

62 'NATO Publishes a How-to Manual for Cyber Warfare' (19 March 2013), available at www.digitaltrends.com/cool-tech/natos-cyberwar-rules-leave-the-civilians-out-of-it.

63 Statement by Colonel Kirby Abbott, assistant legal adviser at Nato, in 'Rules of Cyberwar' *supra* note 60.

64 H. Koh, 'International Law in Cyberspace', *USCYBERCOM Inter-Agency Legal Conference* (18 September 2012), available at www.state.gov/s/l/releases/remarks/197924.htm. According to Schmitt, 'since the speech had been fully cleared in the inter-agency process, it can be viewed as expressing the US government views on the issues'. M. Schmitt, 'International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed', (2012) 54 *Harvard Law Journal* 13, at 14.

65 See Schmitt, ibid., at 15.

66 In relation to scientific expertise this point was made by, inter alia, Ulrich Beck, 'a different computer, a different specialist, a different institute – a different "reality". It would be a miracle if it did not already exist, a miracle and not science'. See U. Beck, *Risk Society* (1992), at 166.

international legal rules. Anyone now claiming that (s)he knows with certainty that a rule should be applied in a particular way, can be confronted with the existence of a lack of consensus between reputable experts on the application of the very same rule ('who are you to claim that you know better than the experts who could not agree?'). In this context, it is interesting to note that the Tallinn Manual also critiques the ICRC expert study on direct participation in hostilities, with some experts arguing that the ICRC interpretation of what constitutes 'direct' participation 'makes little operational sense'.[67] Also within the Manual itself, opposing views are presented, for example, when it comes to fundamental issues such as the applicability of the laws of armed conflict. As the Manual makes clear, experts disagree on the conditions of applicability of the laws of armed conflict and could not reach consensus on the qualification of the Stuxnet attack against Iran in 2010.[68] Similarly, the Manual officially presents disagreement between experts on the definition of an armed conflict,[69] the territorial limitations to the laws of armed conflict,[70] and the distinction between international and non-international armed conflicts.[71]

Second, experts can reach consensus that a rule is too underdetermined to draw any definite conclusions regarding its concrete application. Such an official presentation of underdeterminacy weakens the position of anyone claiming that the rule should be read and applied in a particular fashion. Below, we will give one more elaborate example of the way in which the Tallinn Manual officially stamps uncertainty regarding international legal rules: the interpretation of the prohibition on the use of force (section 3.2). The prohibition on the use of force is generally considered as one of the cornerstones of the UN framework, and of post-1945 international law in general.[72] At the same time, the precise meaning and scope of Article 2(4) remains unclear and subject to much controversy. The Tallinn experts were thus called to apply an undetermined, yet pivotal, provision of international law to the field of cyberspace.

### 3.2. Use of force

One of the core questions in relation to cyberattacks is whether – and under what conditions – they can qualify as 'uses of force' as prohibited by Article 2(4) of the UN Charter and international customary law. From the outset, the Tallinn Manual makes clear that the capacity to deal with cyberattacks via Article 2(4) is limited, since the prohibition on the use of force is directed to states only. Cyberattacks by non-state groups are therefore beyond the scope of this prohibition, unless they can be attributed to a state.[73] However, even if it were possible to attribute a cyberoperation to a state, it would still be difficult to determine whether this operation actually qualifies

67 Rule 35, under 10. Note that this critique reflects the position of Michael Schmitt who initially participated and eventually withdrew from the ICRC project precisely because it failed to strike a proper balance between humanity and military necessity. See *supra* note 1.
68 Rule 22, under 12–14, see also section 2.2 above
69 Rule 20, under 5.
70 Rule 21, under 3.
71 Rule 22, under 9; Rule 23, under 3
72 B. Simma et al., *The Charter of the United Nations: A Commentary* (2002).
73 Rule 10, under 5.

as 'force' under Article 2(4). Absent a definition of 'force' in international law, those who are bound to interpret and apply the term need to makes use of interpretative strategies such as analogies and teleological and systematic understandings. This is exactly what the Tallinn Manual does when linking the prohibition on the use of force to cyberoperations.

First of all, it applies by analogy the 'scale and effects' test that the International Court of Justice used in *Nicaragua* to determine whether an intervention constitutes an 'armed attack' giving rise to self-defence. While the Manual accepts the difference between the terms 'use of force' and 'armed attack',[74] it regards the 'scale and effects' criterion as useful to distinguish 'acts that qualify as uses of force from those that do not'.[75] This test, however, still leaves much room for interpretation when applied to concrete situations. While the Manual acknowledges this,[76] it also makes an unusual attempt to reduce the uncertainty surrounding the scope of the prohibition on the use of force. The Manual states that 'the International Group of Experts took notice of an approach that seeks to assess the likelihood that States will characterize a cyberoperation as a use of force'.[77] What follows in the report is a list of factors that states could take into account, factors that are taken from an article by the chairman of the Tallinn group of experts written some 14 years ago.[78]

At first sight, it may seem that the inclusion of this list of factors helps to reduce uncertainties regarding the application of the prohibition on the use of force to cyberoperations. In its current formulation, however, it is more likely that the inclusion will produce the opposite effect: it officially stamps the uncertainties surrounding the scope of the prohibition in the context of cyberattacks. This is not just because the factors themselves are unavoidably phrased in language that still leaves room for different interpretations. There are three more fundamental reasons why the report reintroduces uncertainty through its invocation of expertise.

First, the status of the factors themselves remains highly uncertain. They are clearly not presented as reflective of the *opinio juris* of states and are not derived from the established sources of international law. Instead, they are presented as empirical in nature, as 'factors that influence States making use of force assessments'.[79]

---

74 As may be recalled, the Court regarded an armed attack (as mentioned in Art. 51 of the UN Charter) as 'one of the most grave forms of use of force', that gives rise to a right to self-defense for the victim state. In order to determine whether a use of force is of such magnitude as to constitute an armed attack, the Court used the 'scale and effects' test: it examined the consequences of a particular use of force in order to determine whether it also constitutes an armed attack.

75 Rule 11, under 1.

76 See, for example, the way in which the Manual deals with the question whether affording sanctuary amounts to an illegal use of force under international law. A majority (in other words, not all members) answered this in the negative, but added that 'the provision of sanctuary coupled with other acts, such as substantial support or providing cyber defences for the non-State group *could, in certain circumstances*, be a use of force' (my italics). What the 'could' and the 'certain circumstances' entail is not spelled out further.

77 Rule 11, under 8. Note that the Manual uses the careful formulation 'took notice'. The rest of the text, however, does more than just 'noticing': it takes up the approach as an apparently useful tool in assessing cyberattacks.

78 M. N. Schmitt, 'Computer Networks and the Use of Force in International Law: Thoughts on a Normative Framework', (1999) 37 *Columbia Journal of Transnational Law* 885, at 914. The factors include: severity of the attack, immediacy of the response, directness of the link between the attack and the harm done, invasiveness of the attack, measurability of the effects, military character of the attack, state involvement in the attack, presumptive legality of actions under international law generally.

79 Para. 9.

However, the factors are not derived from empirical research either. Instead, they follow from a more intuitive approach spelled out in earlier academic articles by the director of the group of experts, Michael Schmitt. The validity of these criteria, in other words, rests on the intuition, experience, and professionalism of its members, more than on independent sources that provide independent backing. This raises the question why states would follow these intuitions regarding the factual behaviour of states when confronted with normative questions regarding the scope of application of the prohibition on the use of force. States should do so, the Manual argues, because they 'must be highly sensitive to the international community's probable assessment of whether operations violate the prohibition on the use of force'.[80] This, however, only raises the question regarding the nature of the factors identified. Should states take them into account because they already have normative force, as they reflect *opinio juris*? Or should states do so out of self-interest, because they will otherwise run the risk of adverse consequences? Or should the factors be regarded as an attempt to seduce states to start developing customary law along the lines suggested by the Manual? And irrespective of the answers to these questions, why would states follow recommendations not based on empirical or normative research, but on the intuition of experts?

Second, the factors themselves are quite radically relativized in the Manual. The Manual argues that the factors are not to be taken as exhaustive and that states 'depending on the circumstances may look to others, such as the prevailing political environment, whether the operation portends the future use of military force and the identity of the attacker, any record of cyberoperations of the attacker'.[81] By bringing in the political environment, risk assessments, and conjectures as to the status of the attacker, the Manual quite explicitly moves legal considerations into the realm of political deliberation and contextual analysis. Rather than providing pre-given criteria against which political actions can be assessed, the Manual makes the scope of the prohibition on the use of force dependent on unspecified circumstances such as the 'prevailing political environment'. Indeed, this may very well be a correct empirical analysis. However, as parts of an expert group on international law it reads as an official stamping of the radical uncertainties that surround one of the cornerstone provisions of the UN Charter.

## 4. Conclusion

Cyberspace is increasingly imagined in terms of threats to critical infrastructure and discussed in terms of war and military strategy. The threats associated with cyberspace, however, are difficult to manage in terms of the established vocabularies in international law and politics. Strategies such as deterrence or containment are as problematic in answer to cyberthreats as are many of the classical distinctions and principles that underpin international conflict and security law. The advent of cybersecurity as 'policy goal', in other words, has created new complexities and

80 Para. 9.
81 Para. 10.

uncertainties insofar as these do not fit our traditional distinctions of public and private or domestic and international. Hence, most of the uncertainties are framed in terms of risks. The question is thus raised how these uncertainties are reduced by a legal vocabulary, which is centred around norms, and how this creates power relations and touches upon question of authority and legitimacy. In this article we have examined one of the answers to the rise of new uncertainties related to cyberspace: the establishment of international groups of legal experts, who are called upon to apply existing law to the threats associated with cyberwar. The most recent example is that international group of legal experts established through NATO, whose findings have been laid down in the Tallinn Manual on Cyberwar.

The Tallinn Manual reflects many of the paradoxes that inform the use of legal expertise as a way of absorbing uncertainties. The authority of the Manual is claimed to rest on both personal and impersonal sources, both on the specific characteristics of the individual members of the group and on allegedly impersonal sources of law. In terms of outcomes, the Manual reduces uncertainty through consensus on some issues, but also reproduces or even radicalizes uncertainty: it makes authoritative claims in the absence of consensus on the proper interpretation of rules and principles and reintroduces open-ended principles and contextual factors in legal reasoning. The net effect is that the Tallinn Manual often reflects and solidfies rather than reduces the uncertainties that come with issues of cyberwar.